

# Industrial Network Security for SCADA, Automation, Process Control and PLC Systems



# OVERVIEW

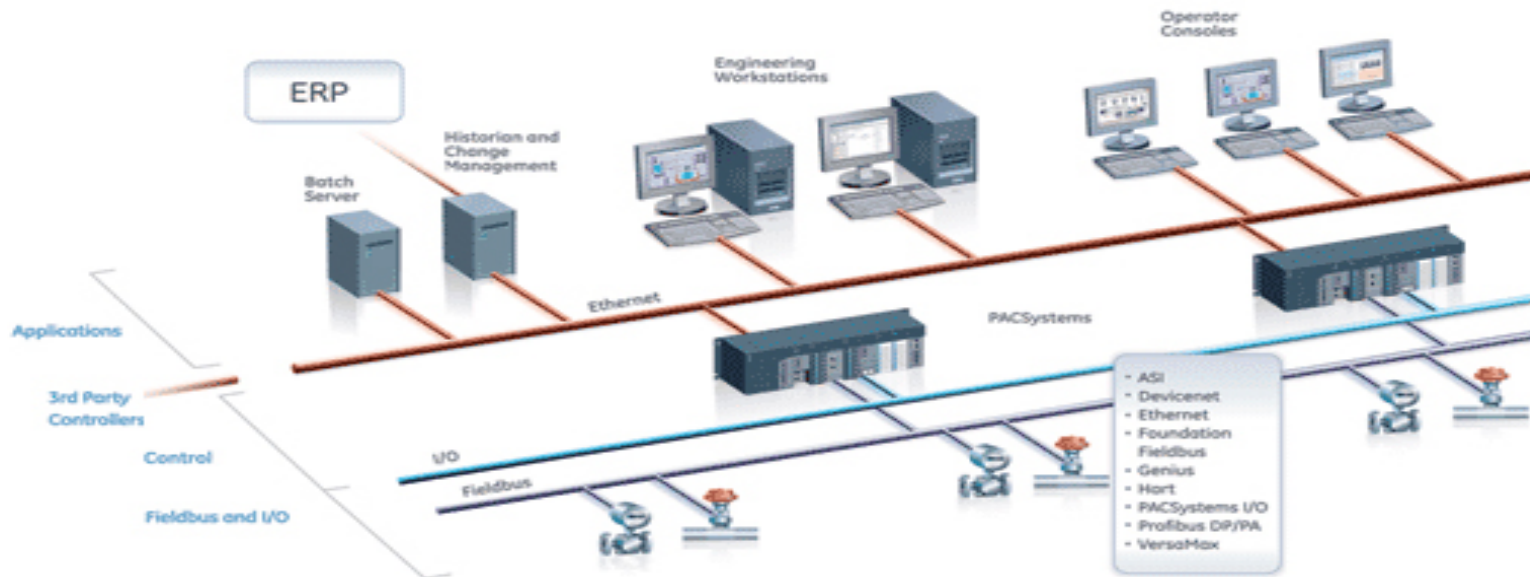
- What is a network?
- Evolution of Networks
- Network Security requirements
- Security in Industrial Automation systems
- Wireless networks
- Industrial Networks and Business Networks-  
*similarities and differences*
- Organisational issues in security
- Security measures
- Security Testing

# WHAT IS A NETWORK?

- An interconnected system of computers
- Communication through specific protocols
- Physical connectivity through copper/optical fiber or by wireless media.
- Vendor independence through standardization
- Better Return On Investment
- Local (LAN), Metro (MAN) or Wide Area (WAN) networks
- Hardware and communication path redundancies in WAN and MAN
- Dedicated links or public data communication networks

# WHAT ARE INDUSTRIAL NETWORKS?

- A network of Programmable controllers (PLC)
- Distributed Control Systems (DCS)
- Supervisory control and Data Acquisition (SCADA) systems



# NETWORK SECURITY

- Analogous to security in the physical world
- Unauthorized access
- 'Loss of Integrity'
- 'Denial Of Service'
- How do you ensure security?
  - Prevent a break-in, put locks
  - Have alarms to warn that a break-in has occurred



# THE BASIC SECURITY ELEMENTS



**Confidentiality**  
**Integrity**  
**Availability**

# PRESENT SECURITY SCENARIO

- Dedicated networks are safe but expensive
- The Internet is cheaper but comes with security risks
- Threats from External and Internal users
- Motivation is political / monetary /or 'thrills'
- Widespread system knowledge
- Easy availability of tools for mounting attacks.
- Protocol/ OS/Application and Human vulnerabilities

# INDUSTRIAL NETWORK SECURITY ISSUES

- Proprietary hardware and software
- Now giving way to open systems  
Ex: HMI and Database systems
- Interconnection between Industrial and business networks
- TCP/IP protocol in Industrial automation
- Access to Internet from corporate networks



# WIRELESS NETWORKING

- Wireless networking becoming popular
  - Mobile users (laptops/palmtops) within a campus
  - Remote monitoring and control applications
- Examples:** Pump control, weather data collection
- EASY to intercept Wireless signals
  - Internet connectivity at public places through wireless
  - Vulnerabilities of wireless now added to those of Internet

# SIMILARITIES BETWEEN INDUSTRIAL AND BUSINESS NETWORKS

- Same owners and general goals
- Same technologies (Ethernet, TCP/IP, Windows, etc.)
- Common facilities
- Interconnected at one or more points

**As a result:**

Security approach of both types of networks have a lot of similarities.

# AND THE DIFFERENCES?

## **Industrial Networks:**

Reliability and Response time and safety

Better security through proprietary operating systems

## **Business networks**

Availability and delivery of service.

Different Risk management goals

# ORGANIZATIONAL ASPECTS OF SECURITY

- Security is NOT just a matter of technology.
- Needed: A clearly defined organisational security policy.
- What is the probability of a security incident?
- What are its risks?
- What is the cost for security systems, training and periodic testing.
- Get the users to understand and cooperate

# NETWORK SECURITY MEASURES

- Authentication, Authorization and Accounting (AAA)
- Encryption of data
- Routers and Firewalls for access control and filtering
- Intrusion detection and response
- VLANs as a security solution for LANs
- Secure Virtual private Networks for remote user access



# SECURITY TESTING

Testing ensures that the security implementation is effective and follows organizational security policies.

## **The issues:**

When to test?

What tests to conduct?

How frequently?

On which systems?

Who is responsible and for what?

**How much will it cost?**

# CONCLUSION

- Common aspects in the security of Industrial and business networks
- Important: Both Organizational and technical aspects of security
- Testing of security measures at periodic intervals for continued effectiveness



# DO YOU WANT TO KNOW MORE?

If you are interested in **further training** or **information**,  
please visit:

[\*\*http://idc-online.com/slideshare\*\*](http://idc-online.com/slideshare)

